VZCZCXYZ0000
OO RUEHWEB

DE RUEHBJ #0721/01 0600337
ZNR UUUUU ZZH
O 290337Z FEB 08
FM AMEMBASSY BEIJING
TO RUEHC/SECSTATE WASHDC IMMEDIATE 5368
INFO RUEHUL/AMEMBASSY SEOUL IMMEDIATE 0563
RUEHKO/AMEMBASSY TOKYO IMMEDIATE 1824
RUEHMO/AMEMBASSY MOSCOW IMMEDIATE 8947

UNCLAS BEIJING 000721

SIPDIS

SENSITIVE
SIPDIS

E.O. 12958: N/A
TAGS: OTRA AMGT KNNP PREL MNUC KN CH
SUBJECT: COUNTRY CLEARANCE APPROVAL FOR EAP/K SUNG KIM, NSC PAUL HAENLE FEB 29-MAR 2 TO BEIJING

REF: STATE 20266

¶1. (SBU) Embassy Beijing welcomes and grants country clearance February 29 - March 2, 2008, for EAP/K Director Sung Kim and NSC Asia Director Paul Haenle to Beijing for consultations related to the Six-Party Talks.

¶2. (SBU) Political Control Officer:
Nancy Leou, Political Officer
Tel: (86-10)6532-3831 x6040
Cell: (86)139-1023-4347
Fax: (86-10)6532-6423
Unclass E-mail: LeouNW@state.gov

SIPDIS

Control officer will meet travelers at the airport and take them to their hotel.

¶3. (SBU) Hotel reservations have been made at the Grand Hyatt Hotel.

Grand Hyatt Hotel
Beijing Oriental Plaza
1 Dong Changan Jie, Beijing 100738
Ph: (86-10)8518-1234
Fax: (86-10)8518-0000

Security and Threat Assessment

¶4. (U) The threat level for all China posts is considered low for crime and medium for terrorism.

¶5. (U) The Regional Security Office is not aware of any specific threat directed against any U.S. person or traveling delegation. Should such information be developed, the Chinese security services are committed to advise the Embassy of pertinent information and to provide necessary security coverage.

¶6. (U) China experiences a moderate rate of crime, including recent incidents ranging from petty theft to murder. Pickpockets are particularly active in crowded markets and foreigners are often sought out as primary targets. Petty theft from hotel rooms is uncommon, but visitors are advised not to leave valuables lying loose or unattended in their rooms. It is the policy of this Mission that employees, their family members and official visitors to China must not knowingly purchase counterfeit or pirated products during their stay in China. Also, foreigners may be

approached in tourist areas by individuals seeking to exchange U.S. dollars or to sell pirated or fake products, such as compact discs, in violation of intellectual property rights laws. These transactions are illegal, violate post policy, and must be avoided.

¶7. (U) All U.S. citizen personnel serving under Chief of Mission authority in a temporary duty status of 30 days or more must complete appropriate overseas personal security training prior to travel (04 State 66580). Employees who have completed the Security Overseas Seminar Course at State's Foreign Service Institute (FSI) after June 1, 2000 meet this requirement. All other TDYers must either 1) complete the approved four-day seminar at FSI entitled "Serving Abroad for Families and Employees" (SAFE) or 2) have their agency certify to the State Department Bureau of Diplomatic Security that the employee has undergone equivalent security training. The contact for this certification is Assistant Director of Training, DS/T, at telephone (703) 205-2617. Country clearance will not be granted for any traveler with planned TDY in excess of 30 days if this information is not stated/certified. POC for additional information is DS_RSO, Beijing at: ds_rso_Beijing@state.gov(Note: Travelers from DHS/CBP, DIA, FBI, DOD, and the Peace Corp have been pre-certified by their agencies with DS.)

¶8. (U) All/all official visitors are required to obtain a pre-departure, country specific counterintelligence briefing from their parent agency before departing for China. Visitors should contact the security office of their parent agency. If the parent agency is unable to give the briefing or needs assistance/guidance, the visitor should contact the Bureau of Diplomatic Security's Division of

Counterintelligence (DS/ICI/CI) at 571-345-7641, 3966, or 3968 to schedule a briefing. HQ DS/CI is located at SA-20, 1801 Lynn St., Rosslyn, Virginia 20522-2008. Department of State personnel should contact the DS/ICI/CI directly to schedule a briefing. Official visitors may also be required to attend a post specific security briefing upon their arrival in country. The type of briefing is contingent on the length of the planned visit. Upon arrival in Beijing, all TDY personnel should contact the Regional Security Office at 6532-3831, ext. 6036 to determine level of briefing required.

¶9. (U) Visitors are reminded to take necessary precautions in safeguarding sensitive material and information. All non-USG facilities must be considered technically compromised and may not be used to discuss, process, or store classified information. Telephone calls, e-mail, and Internet usage are routinely monitored and hotel rooms searched.

¶10. (U) All TDY U.S. citizen employees of the U.S. Government, civilian or military, who are under the authority of the Chief of Mission are subject to the reporting requirement stated in 12 FAM 262 regarding contact reports, i.e. any initial (non-business related) contact with a national from a country with a Critical threat (counterintelligence) post, as listed on the Department's Security Environment Threat List (SETL), must be reported. In general, employee reporting should occur within one business day after such contact has occurred. If unable to report within this time frame, or unsure about the need to report at all, employees should contact the RSO or PSO as soon as practicable. If the RSO/PSO is unavailable, notify the Management Officer or the Deputy Chief of Mission.

¶11. (U) Per 12 FAM 262, this reporting requirement generally applies whenever:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(2) The employee is concerned that he or she may the target of actual or attempted exploitation by a foreign entity.

(3) That national attempts to establish recurring contact or seems to be actively seeking a close personal association, beyond professional or personal courtesies.

¶12. (U) Travelers should be aware that previous visitors have reported that their unattended computers have been subjected to tampering. The efforts may be directed toward obtaining information on the computers, but problems ranging from viruses left on their systems to hard drives, which are no longer functional, have been reported. Hotels and private Chinese Internet providers have in some cases given hotel guests "free" thumb drives for use with their computers. The source and quality of these devices are unknown. Such devices could contain malicious codes and viruses and should not be used on government computers. Official visitors are reminded that non-inspectable electrical/electronic equipment, i.e., cellular telephones, laptop computers, personal digital assistants (PDAs), etc., may not be brought into the controlled access areas of the Chancery. If a visitor intends to travel with USG-owned computers and equipment for use within the chancery, please contact the Regional Security Officer at 86-10-6532-3831 ext. 6058, or GormanB2@state.gov or MooreBM@state.gov, for information and guidelines.

¶13. (U) Additionally, all classified and sensitive materials must be secured at the Embassy upon arrival in country. All classified material must be brought into China via diplomatic pouch.

¶14. (U) Travelers must contact the Embassy or nearest Consulate General upon arrival in China and provide telephone and address information while in country.

¶15. (U) Passports and visas are required. Americans arriving/transiting without valid passports and Chinese visas are not permitted to enter China and may also be subject to fines. Visas are required to transit China on the way to and from Mongolia or North

Korea. Those visitors traveling to China on a single entry visa should be reminded that trips to Hong Kong or Macau Special Administrative Regions are treated as a visit outside Mainland China. If the traveler is planning to return to Mainland China after a visit to one of these two destinations on the same single entry visa, they will be denied entry. Visitors facing this dilemma will be required to apply for a new visa at the Chinese consulate in Hong Kong to gain re-entry into Mainland China.

RANDT